UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,954	09/03/2004	Alexander Shipp	117-512	1417

23117 7590 06/04/2009

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER
BROMELL, ALEXANDRIA Y

ART UNIT	PAPER NUMBER
2167	

MAIL DATE	DELIVERY MODE
06/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/500,954	SHIPP, ALEXANDER	
	Examiner	Art Unit	
	ALEXANDRIA Y. BROMELL	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 - 2, 5 - 8, and 11 - 16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 - 2, 5 - 8, and 11 - 1* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 July 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments, see Remarks, filed January 30, 2009, with respect to the rejection(s) of claim(s) 1 – 2, 5 – 8, and 11 - 16 under 35 U.S.C. 102(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Ivan Teblyashkin et al. (EP 1291749), hereinafter, "Teblyashkin," in view of Neil Cowie et al. (GB 2378015), hereinafter, "Cowie."

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 – 2, 5 – 8, and 11 – 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ivan Teblyashkin et al. (EP 1291749), hereinafter, "Teblyashkin," in view of Neil Cowie et al. (GB 2378015), hereinafter, "Cowie."

With respect to claim 1, Teblyashkin teaches a) a computer database containing records of known executable programs which are deemed to be not malware and criteria by which a file being processed can be determined to be an instance of one of those programs, the criteria including at least one characteristic signature associated with each said instance (i.e. computer files that are known to not be malware are compared with files possibly infected by a virus using matching characteristic blocks,

column 1, lines 44 - 56), b) means for processing a file being transferred between computers, the means b) comprising a file recognizer operative to determine whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said at least one characteristic signature associated with the said instances (i.e. computer program files are checked to determine if they have infected blocks, column 1, lines 44 – 56, figure 4), and a difference checker operative, in the case that the file recognizer determines the file being processed to be an instance of a known program, to check whether the file is an unchanged version of that known program (i.e. the version of the program is checked to see if it is conflicting with the correct program version, indicating presence of possible malware, column 3, lines 9 - 17).

Teblyashkin does not explicitly disclose the means for signaling the file.

However, Cowie teaches c) means for signaling the file, depending on the determination made by the processing means, as being likely to be not malware if it is an unchanged version of a known file (i.e. if the file is an unchanged version, it is unlikely malware, page 9, lines 10 - 22), likely to be malware if it is a changed version of a known file (i.e. file is likely to be malware if its version is changed, page 9, lines 6 - 10, figure 6), or of unknown status if it is not determined as being an instance of a known file (i.e. file status may be unknown, page 9, lines 6 - 10).

Teblyashkin and Cowie are analogous art because they are from the same field of endeavor of scanning programs to detect possible malware.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to modify the teachings of Teblyashkin with the teachings of Cowie in order to efficiently detect the presence of trojans and worms using signature scanning techniques (Cowie, page 1, lines 13 - 22).

With respect to claim 2, Teblyashkin teaches a computer program product for automatically generate virus fingerprint data for use in detecting computer files infected with a computer virus (column 1, lines37 - 42). Teblyashkin does not explicitly disclose the means for signaling the file.

However, Cowie teaches d) means for processing a file being transferred between computers to determine whether it is considered to be, or considered possibly to be, malware, and wherein the means d) is operative to subject a file to processing if the file is signaled by the signaling means c) as being of unknown status (i.e. when the system checks the fingerprints of the file and determines them to be unknown status, the fingerprints are processed and tested, page 9, lines 1 - 22).

Teblyashkin and Cowie are analogous art because they are from the same field of endeavor of scanning programs to detect possible malware. At the time of the invention, it would have been obvious to one of ordinary skill in the art to modify the teachings of Teblyashkin with the teachings of Cowie in order to efficiently detect the presence of trojans and worms using signature scanning techniques (Cowie, page 1, lines 13 - 22).

With respect to claim 5, Teblyashkin teaches a computer program product for automatically generate virus fingerprint data for use in detecting computer files infected with a computer virus (column 1, lines37 - 42). Teblyashkin does not explicitly disclose the means for signaling the file.

However, Cowie teaches the difference checker is operative to generate a checksum for the entire file under consideration or for at least one selected region thereof, and to compare the checksum or checksums with those of entries in the database (i.e. checksum values are compared, page 3, lines 17 – 18, page 6, lines 20 – 31, page 7, lines 1 - 14).

Teblyashkin and Cowie are analogous art because they are from the same field of endeavor of scanning programs to detect possible malware. At the time of the invention, it would have been obvious to one of ordinary skill in the art to modify the teachings of Teblyashkin with the teachings of Cowie in order to efficiently detect the presence of trojans and worms using signature scanning techniques (Cowie, page 1, lines 13 - 22).

With respect to claim 6, Teblyashkin teaches a computer program product for automatically generate virus fingerprint data for use in detecting computer files infected with a computer virus (column 1, lines37 - 42). Teblyashkin does not explicitly disclose the means for signaling the file.

However, Cowie teaches including an exception list handler operative to determine, in relation to a file which the processing means b) has determined is a changed version of a known file, whether that file has characteristics matching an entry

in an exception list of files, the signaling means c) being operative to signal the file as malware only if it is not in the exception list or as being of unknown status otherwise (i.e. program fingerprints are analyzed to determine if the program file contains malware, and if processing should continue, page 9, lines 10 - 22).

Teblyashkin and Cowie are analogous art because they are from the same field of endeavor of scanning programs to detect possible malware. At the time of the invention, it would have been obvious to one of ordinary skill in the art to modify the teachings of Teblyashkin with the teachings of Cowie in order to efficiently detect the presence of trojans and worms using signature scanning techniques (Cowie, page 1, lines 13 - 22).

With respect to claim 7, Teblyashkin teaches maintaining a computer database containing records of known executable programs which are deemed to be not malware and criteria by which a file being processed can be determined to be an instance of one of those programs, the criteria including at least one characteristic signature associated with each said instance (i.e. computer files that are known to not be malware are compared with files possibly infected by a virus using matching characteristic blocks, column 1, lines 44 - 56), processing a file being transferred between computers by determining whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said at least one characteristic signature associated with the said instances (i.e. computer program files are checked to determine if they have infected blocks, column 1, lines 44 – 56, figure 4), and checking, in the case that the file recognizer determines the file being processed to

be an instance of a known program, to check whether the file is an unchanged version of that known program (i.e. the version of the program is checked to see if it is conflicting with the correct program version, indicating presence of possible malware, column 3, lines 9 - 17).

Teblyashkin does not explicitly disclose the means for signaling the file. However, Cowie teaches signaling the file, depending on the determination made by the processing means, as being likely to be not malware if it is an unchanged version of a known file (i.e. if the file is an unchanged version, it is unlikely malware, page 9, lines 10 - 22), likely to be malware if it is a changed version of a known file (i.e. file is likely to be malware if its version is changed, page 9, lines 6 - 10, figure 6), or of unknown status if it is not determined as being an instance of a known file (i.e. file status may be unknown, page 9, lines 6 - 10).

Teblyashkin and Cowie are analogous art because they are from the same field of endeavor of scanning programs to detect possible malware. At the time of the invention, it would have been obvious to one of ordinary skill in the art to modify the teachings of Teblyashkin with the teachings of Cowie in order to efficiently detect the presence of trojans and worms using signature scanning techniques (Cowie, page 1, lines 13 - 22).

With respect to claim 8, Teblyashkin teaches a computer program product for automatically generate virus fingerprint data for use in detecting computer files infected with a computer virus (column 1, lines37 - 42). Teblyashkin does not explicitly disclose the means for signaling the file.

However, Cowie teaches processing a file being transferred between computers to determine whether it is considered to be, or considered possibly to be, malware, if the file is signaled by the signaling step c) as being of unknown status (i.e. when the system checks the fingerprints of the file and determines them to be unknown status, the fingerprints are processed and tested, page 9, lines 1 - 22).

Teblyashkin and Cowie are analogous art because they are from the same field of endeavor of scanning programs to detect possible malware. At the time of the invention, it would have been obvious to one of ordinary skill in the art to modify the teachings of Teblyashkin with the teachings of Cowie in order to efficiently detect the presence of trojans and worms using signature scanning techniques (Cowie, page 1, lines 13 - 22).

With respect to claim 11, Teblyashkin teaches a computer program product for automatically generate virus fingerprint data for use in detecting computer files infected with a computer virus (column 1, lines37 - 42). Teblyashkin does not explicitly disclose the means for signaling the file.

However, Cowie teaches the difference checker is operative to generate a checksum for the entire file under consideration or for at least one selected region thereof, and to compare the checksum or checksums with those of entries in the database (i.e. checksum values are compared, page 3, lines 17 – 18, page 6, lines 20 – 31, page 7, lines 1 - 14).

Teblyashkin and Cowie are analogous art because they are from the same field of endeavor of scanning programs to detect possible malware. At the time of the

invention, it would have been obvious to one of ordinary skill in the art to modify the teachings of Teblyashkin with the teachings of Cowie in order to efficiently detect the presence of trojans and worms using signature scanning techniques (Cowie, page 1, lines 13 - 22).

With respect to claim 12, Teblyashkin teaches a computer program product for automatically generate virus fingerprint data for use in detecting computer files infected with a computer virus (column 1, lines37 - 42). Teblyashkin does not explicitly disclose the means for signaling the file.

However, Cowie teaches including an exception list handler operative to determine, in relation to a file which the processing means b) has determined is a changed version of a known file, whether that file has characteristics matching an entry in an exception list of files, the signaling means c) being operative to signal the file as malware only if it is not in the exception list or as being of unknown status otherwise (i.e. program fingerprints are analyzed to determine if the program file contains malware, and if processing should continue, page 9, lines 10 - 22).

Teblyashkin and Cowie are analogous art because they are from the same field of endeavor of scanning programs to detect possible malware. At the time of the invention, it would have been obvious to one of ordinary skill in the art to modify the teachings of Teblyashkin with the teachings of Cowie in order to efficiently detect the presence of trojans and worms using signature scanning techniques (Cowie, page 1, lines 13 - 22).

With respect to claim 13, Teblyashkin teaches maintaining a computer database containing records of known executable programs which are deemed to be not malware and criteria by which a file being processed can be determined to be an instance of one of those programs, the criteria including at least one characteristic signature associated with each said instance (i.e. computer files that are known to not be malware are compared with files possibly infected by a virus using matching characteristic blocks, column 1, lines 44 - 56), processing a file being transferred between computers by determining whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said at least one characteristic signature associated with the said instances (i.e. computer program files are checked to determine if they have infected blocks, column 1, lines 44 – 56, figure 4), and checking, in the case that the file recognizer determines the file being processed to be an instance of a known program, to check whether the file is an unchanged version of that known program (i.e. the version of the program is checked to see if it is conflicting with the correct program version, indicating presence of possible malware, column 3, lines 9 - 17).

Teblyashkin does not explicitly disclose the means for signaling the file. However, Cowie teaches signaling the file, depending on the determination made by the processing means, as being likely to be not malware if it is an unchanged version of a known file (i.e. if the file is an unchanged version, it is unlikely malware, page 9, lines 10 - 22), likely to be malware if it is a changed version of a known file (i.e. file is likely to be malware if its version is changed, page 9, lines 6 - 10, figure 6), or of unknown status if

it is not determined as being an instance of a known file (i.e. file status may be unknown, page 9, lines 6 - 10).

Teblyashkin and Cowie are analogous art because they are from the same field of endeavor of scanning programs to detect possible malware. At the time of the invention, it would have been obvious to one of ordinary skill in the art to modify the teachings of Teblyashkin with the teachings of Cowie in order to efficiently detect the presence of trojans and worms using signature scanning techniques (Cowie, page 1, lines 13 - 22).

With respect to claim 14, Teblyashkin teaches a computer program product for automatically generate virus fingerprint data for use in detecting computer files infected with a computer virus (column 1, lines37 - 42). Teblyashkin does not explicitly disclose the means for signaling the file.

However, Cowie teaches processing a file being transferred between computers to determine whether it is considered to be, or considered possibly to be, malware, if the file is signaled by the signaling step c) as being of unknown status (i.e. when the system checks the fingerprints of the file and determines them to be unknown status, the fingerprints are processed and tested, page 9, lines 1 - 22).

Teblyashkin and Cowie are analogous art because they are from the same field of endeavor of scanning programs to detect possible malware. At the time of the invention, it would have been obvious to one of ordinary skill in the art to modify the teachings of Teblyashkin with the teachings of Cowie in order to efficiently detect the

presence of trojans and worms using signature scanning techniques (Cowie, page 1, lines 13 - 22).

With respect to claim 15, Teblyashkin teaches records for files which are instances of programs determined by the file-scanning system not to be malware are added to the computer database (i.e. new fingerprints are added to the database, column 1, lines 37 - 42).

With respect to claim 16, Teblyashkin teaches that the processor assigns a score to a file identified as likely to be malware (i.e. different codes or scores may be used to identify possible malware, column 5, lines 22 – 26 and 36 - 45).

Conclusion/Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ALEXANDRIA Y. BROMELL whose telephone number is (571)270-3034. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John R. Cottingham can be reached on 571-272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Alexandria Y Bromell/
Examiner, Art Unit 2167
May 30, 2009

/Shahid Al Alam/
Primary Examiner, Art Unit 2162